



Important Advisory – Email Fraud Schemes

In this day and age, it seems that we are always assessing and mitigating risk... *our jobs often revolve around it.* When financial institutions assess their **cybersecurity risk**, the realization that email compromise fraud schemes are a significant vulnerability easily becomes apparent.

Earlier this month, FinCEN issued an **Advisory** focused on criminal activities that are initiated via e-mail to defraud institutions and their customers. As email communication is used every day, by all employees, the access points for fraud can almost be too cumbersome to get your arms around. However, it's important for institutions and employees to understand this risk and prevent it from occurring. The FBI has reported **over \$3 billion in losses** due to business email compromise schemes.

As the Advisory points out, institutions and their security programs can play an important role in identifying, preventing and reporting fraud schemes. While we're familiar with account takeovers where criminals actually conduct transactions, email fraud is initiated by criminals impersonating their victims by either using the victim's email account or creating and using a false-email account that gives the appearance of being the victim's account.

The Advisory highlights that schemes are perpetuated in a variety of ways. Staff should be aware that this could involve the impersonation of:

- **Customers,**
- **Institution Executives and Staff,**
- **Suppliers and Vendors,**
- **Service Professionals such as Brokers or Accountants,**
- **Realtors and**
- **Attorneys.**

Detecting "red flags" is an important component of your cybersecurity program. For example, observing altered email account addresses can help staff identify fraud schemes. The Advisory provides an excellent list of "red flags." The issuance also contains details related to filing a SAR including cyber-related information.

If you would like to read FinCEN's Guidance, you may find Advisory FIN-2016-A003 here - [FinCEN Advisory](#)

Online Compliance Consulting Update!

The Online Compliance Consulting Dashboard has been enhanced!

- **Knowledge Base Updates:**
 - ✓ NEW Compliance Alert - SCRA
 - ✓ UPDATED Compliance Alert – Military Lending Act
 - ✓ 19 NEW Q&As – Military Lending Act
 - ✓ 29 NEW Q&As - SCRA
 - ✓ 11 NEW Q&As – Reg. Z
 - ✓ August 2016 News
- **Important Resource / Tool Updates:**
 - ✓ NEW Compliance for Commercial Lenders Tool
 - ✓ Updated Checklists & Regulatory Deadlines
 - ✓ NEW Links on Rulemaking & Regulations Page

To access this information and all other compliance features, go to: <http://compliance.smslp.com/>

Speaking of Cybersecurity...

We all know that our risks are increasing. You can no longer rely solely on your outsourced vendors to protect your data. Regulators are increasing their focus on your cybersecurity programs and efforts focused on preventing data breaches. **Do you need help using the FFIEC's Cybersecurity Assessment Tool? Are you prepared for regulatory examinations on this crucial issue?**

Depending on your responses to those questions, you may be interested in an upcoming webinar – **Regulatory Oversight of FFIEC's Cybersecurity Assessment: Are you Prepared?** presented by **Gary Deutsch**. If interested, you may find details at Bankers WEB [here](#).

Attention BSA Officers

At the end of August, the **Department of the Treasury**, along with the **FRB, FDIC, NCUA, OCC**; issued a fact sheet on **foreign correspondent banking** – an approach to BSA/AML and OFAC sanctions supervision and enforcement.

Institutions that maintain correspondent accounts for foreign financial institutions are required to establish appropriate, risk-based due diligence programs that are designed to manage the risks with these relationships. The fact sheet provides the following:

- A summary of key aspects of supervisory and enforcement strategy for correspondent banking;
- A description of expectations for institutions;
- Information on enforcement actions, including civil money penalties; and
- An explanation of the important role of FinCEN and OFAC.

The press release may be found [here](#).

Complaint Snapshot

In a recent press release, the CFPB issued a monthly **snapshot of consumer complaints** about bank accounts and services, which reflects ongoing problems that consumers are experiencing. Of note, the type of bank account that generates the most complaints is a checking account and the most common issue identified is tied to account management.

The report also includes a bullet point list of detailed categories and problems consumers are experiencing, that includes **overdraft programs, availability of funds and promotional offerings**.

We recommend reviewing this report, as it highlights areas that are found to be problematic. The press release and report can be found [here](#).



NEW DATE!! Mark your calendar for our next **Be Prepared!** Compliance Update webinar. It is scheduled for **September 27, 2016**.

Details can be found on BankersWEB, [here](#).

Convenient and Affordable Compliance Assistance

Do you need help preparing for the upcoming regulatory requirements? SC+S can help with our Online Compliance Consulting services, which combines the ease of online tools with the guidance of a compliance expert.

You will have access to an online compliance expert who will:

- Answer all of your compliance questions;
- Review your new policies and disclosures for compliance; and
- Train your Board of Directors on upcoming regulatory requirements.

You will also receive access to our online tools, including:

- Our Compliance Calendar;
- Our Dashboard Feature and Progress List, that enables you to determine what steps you will need to take to comply with the requirements and track your progress as you implement them;
- Our exclusive Knowledge Base of compliance Q&As; and
- FREE access to our quarterly Be Prepared! webinar series on upcoming regulatory requirements.

For more information or a free demo, contact Rhonda Coggins at 512-703-1509.

Contact Us

Sheshunoff Consulting + Solutions

901 S. Mopac Expressway
Barton Plaza V, Suite 140
Austin, TX 78746

© 2016 SCSR, L.L.C.

You have received this newsletter as either a complement to other SC+S services you receive, or in response to your request. If you no longer wish to receive this newsletter, please send an email to compliance@smslp.com.

No further reproduction or distribution is allowed outside your organization without permission.